

1
2 **CLAIMS:**

3 1. A computer-readable medium having computer-executable
4 instructions that, when executed by the system, performs a method comprising:

5 obtaining a message M ;

6 defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing
7 function of the message;

8 calculating a private key α in accordance with this equation
9
$$\alpha = \sum_{i=1}^n v_i \alpha_i \bmod m;$$

10 producing a signature S in accordance with this equation: $S = \alpha H_2(M)$,
11 where $H_2(M)$ is a predefined second hashing function of the message;

12 indicating results based, at least in part, on the obtaining, defining,
13 calculating, or producing.
14

15 2. A medium as recited in claim 1, wherein the results of the indicating
16 comprises a message-and-signature pair (M, S) .
17

18 3. A medium as recited in claim 1, wherein the results of the indicating
19 comprises a message-and-signature pair $(M, \mu S)$ and the method further comprises
20 calculating $\mu = H_3(BK, M)$, where BK is key and $H_3(BK, M)$ maps M into an
21 integer within a defined range.
22
23
24
25

1 4. A medium as recited in claim 1, wherein the α_i are scaling factors for
2 n discrete logs of $\alpha_1 P, \dots, \alpha_n P$ base P , where n is a positive integer, P is a point
3 on an elliptic curve and a public key.

4
5 5. A medium as recited in claim 1, wherein
6 α_i are scaling factors for n discrete logs of $\alpha_1 P, \dots, \alpha_n P$ base P , where n is
7 a positive integer, wherein P is a point on an elliptic curve;
8 a point P is of order m and where $e_m(P, Q) : E[m] \times E[m] \rightarrow GF(q)^*$ denotes
9 a Tate or Weil or Squared Tate or Squared Weil Pairing, where $\alpha_1 P, \dots, \alpha_n P =$
10 Q_1, \dots, Q_n and where q is a prime power.

11 6. A medium as recited in claim 1, wherein the signature S is
12 represented by a number of bits, wherein the method further comprises truncating
13 a specific number of bits off of S before the indicating.

14
15 7. A medium as recited in claim 1, wherein the first hashing function
16 produces values in $\{\pm 1\}$.

17
18 8. A computing device comprising:
19 an output device;
20 a medium as recited in claim 1.

1
2 **9.** A computer-readable medium having computer-executable
3 instructions that, when executed by the system, performs a method comprising:

4 choosing n discrete logs of $\alpha_1 P, \dots, \alpha_n P$ base P , where n is a positive
5 integer, P is a point on an elliptic curve and a public key, and α_i is a scaling factor
6 and a private key;

7 indicating results of the choosing.

8
9 **10.** A medium as recited in claim 9, wherein a point P is of order m
10 and where $e_m(P, Q) : E[m] \times E[m] \rightarrow GF(q)^*$ denotes a Tate or Weil or Squared Tate
11 or Squared Weil Pairing, where $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$ and where q is a prime
12 power.

13
14 **11.** A medium as recited in claim 9 further comprising generating a
15 digital signature based upon a message M and α_i .

16
17 **12.** A computing device comprising:
18 an output device;
19 a medium as recited in claim 9.

1 13. A method facilitating the production of a digital signature, the
2 method comprising:

3 obtaining a message M ;

4 defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing
5 function of the message;

6 calculating a private key α in accordance with this equation

7
$$\alpha = \sum_{i=1}^n v_i \alpha_i \text{ mod } m;$$

8 producing a signature S in accordance with this equation: $S = \alpha H_2(M)$,
9 where $H_2(M)$ is a predefined second hashing function of the message;

10 indicating results based, at least in part, on the obtaining, defining,
11 calculating, or producing.

12
13 14. A method as recited in claim 13 wherein the results of the indicating
14 comprises a message-and-signature pair (M, S) .

15
16 15. A method as recited in claim 13, wherein the results of the indicating
17 comprises a message-and-signature pair $(M, \mu S)$ and the method further comprises
18 calculating $\mu = H_3(BK, M)$, where BK is key and $H_3(BK, M)$ maps M into an
19 integer within a defined range.

20
21 16. A method as recited in claim 13, wherein the α_i are scaling factors
22 for n discrete logs of $\alpha_1 P, \dots, \alpha_n P$ base P , where n is a positive integer, P is a
23 point on an elliptic curve and a public key.

1 17. A method as recited in claim 13, wherein
2 α_i are scaling factors for n discrete logs of $\alpha_1 P, \dots, \alpha_n P$ base P , where n is
3 a positive integer, P is a point on an elliptic curve;

4 a point P is of order m and where $e_m(P, Q) : E[m] \times E[m] \rightarrow GF(q)^*$ denotes
5 a Tate or Weil or Squared Tate or Squared Weil Pairing, where $\alpha_1 P, \dots, \alpha_n P =$
6 Q_1, \dots, Q_n and where q is a prime power

7 18. A method as recited in claim 13, wherein the signature S is
8 represented by a number of bits, wherein the method further comprises truncating
9 a specific number of bits off of S before the indicating.

10
11 19. A method as recited in claim 13, wherein the first hashing function
12 produces values in $\{\pm 1\}$.

1
2 20. A computer-readable medium having computer-executable
3 instructions that, when executed by the system, performs a method comprising:

4 obtaining an input message-and-signature pair (M, S) ;

5 defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing
6 function of the message;

7 calculating a point Q on an elliptic curve in accordance with this equation:

8
$$Q = \sum_{i=1}^n v_i Q_i;$$

9 comparing pairing outputs of a pair (P, S) and a pair $(Q, H_2(M))$, where
10 $H_2(M)$ is a predefined second hashing function of M and P is a point on the elliptic
11 curve;

12 indicating results of the comparing.
13

14 21. A medium as recited in claim 20 further comprising verifying the
15 input message-and-signature pair (M, S) when the indicated results of the
16 comparing is a match.

17
18 22. A medium as recited in claim 20, wherein:

19 the point P being a point on an elliptic curve and of order m and where
20 $e_m(P, Q) : E[m] \times E[m] \rightarrow GF(q)^*$ denotes a Tate or Weil or Squared Tate or Squared
21 Weil Pairing, where $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$ and where q is a prime power

22 the α_i being scaling factors for n discrete logs of $\alpha_1 P, \dots, \alpha_n P$ base P , where
23 n is a positive integer,
24
25

1 **23.** A medium as recited in claim 20, wherein the method further
2 comprises, when the indicated results of the comparing is not a match, modifying
3 the vector v relative to its previous definition and repeating the defining,
4 calculating, and comparing.

5
6 **24.** A medium as recited in claim 20, wherein the method further
7 comprises:

8 when the indicated results of the comparing is not indicate a match,
9 modifying the vector v relative to its previous definition;

10 repeating the defining, calculating, and comparing;

11 if the indicated results of the comparing still does not a match, then
12 repeating the modifying and the repeating of the defining, calculating, and
13 comparing until the indicated results do match.

14
15 **25.** A medium as recited in claim 20, wherein the method further
16 comprises when the indicated results of the comparing is not a match, repeating
17 the defining, calculating, and comparing with the defining being based upon a
18 predefined third hashing function of the message.

19
20 **26.** A medium as recited in claim 20, wherein the signature S is
21 represented by a number of bits, wherein the method further comprises padding S
22 with a specific number of bits before the defining.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

27. A computing device comprising:
an output device;
a medium as recited in claim 20.

1
2 **28.** A method facilitating the verification of a digital signature, the
3 method comprising:

4 obtaining an input message-and-signature pair (M, S) ;
5 defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing
6 function of the message;
7 calculating a point Q on an elliptic curve in accordance with this equation:
8
$$Q = \sum_{i=1}^n v_i Q_i;$$

9 comparing pairing outputs of a pair (P, S) and a pair $(Q, H_2(M))$, where
10 $H_2(M)$ is a predefined second hashing function of M and P is a point on the elliptic
11 curve;
12 indicating results of the comparing.

13
14 **29.** A method as recited in claim 28 further comprising verifying the
15 input message-and-signature pair (M, S) when the indicated results of the
16 comparing is a match.

17
18 **30.** A method as recited in claim 28, wherein
19 the point P being a point on an elliptic curve and of order m and where
20 $e_m(P, Q) : E[m] \times E[m] \rightarrow GF(q)^*$ denotes a Tate or Weil or Squared Tate or Squared
21 Weil Pairing, where $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$ and where q is a prime power
22 the α_i being scaling factors for n discrete logs of $\alpha_1 P, \dots, \alpha_n P$ base P , where
23 n is a positive integer,
24
25

1 **31.** A method as recited in claim 28 further comprising, when the
2 indicated results of the comparing is not a match, modifying the vector v relative
3 to its previous definition and repeating the defining, calculating, and comparing.

4
5 **32.** A method as recited in claim 28 further comprising:
6 when the indicated results of the comparing is not a match, modifying the
7 vector v relative to its previous definition;
8 repeating the defining, calculating, and comparing;
9 if the indicated results of the comparing still does not a match, then
10 repeating the modifying and the repeating of the defining, calculating, and
11 comparing until the indicated results do match.

12
13 **33.** A method as recited in claim 28 further comprising when the
14 indicated results of the comparing is not a match, repeating the defining,
15 calculating, and comparing with the defining being based upon a predefined third
16 hashing function of the message.

17
18 **34.** A method as recited in claim 28, wherein the signature S is
19 represented by a number of bits, wherein the method further comprises padding S
20 with a specific number of bits before the defining.

1 **35.** A computer-readable medium having computer-executable
2 instructions that, when executed by the system, performs a method comprising:
3 obtaining an input message-and-signature pair (M, S') ;
4 defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing
5 function of the message;
6 calculating a point Q on an elliptic curve in accordance with this equation:
7
$$Q = \sum_{i=1}^n v_i Q_i;$$

8 comparing pairing outputs of a pair (P, S') and a pair $(Q, H_2(M))^\mu$, where
9 $H_2(M)$ is a predefined second hashing function of M and P is a point on the elliptic
10 curve and μ is an integer in a defined range;
11 indicating results of the comparing.

12
13 **36.** A medium as recited in claim 35 further comprising verifying the
14 input message-and-signature pair (M, S') when the indicated results of the
15 comparing is a match.

16
17 **37.** A computing device comprising:
18 an output device;
19 a medium as recited in claim 35.
20
21
22
23
24
25